

Ternary Kloosterman sums using Stickelberger's theorem and the Gross-Koblitz formula

Faruk Göloğlu*, Gary McGuire*, Richard Moloney†
 School of Mathematical Sciences
 University College Dublin
 Ireland

June 10, 2010

Abstract

We give results characterising ternary Kloosterman sums modulo 9 and 27. This leads to a complete characterisation of values that ternary Kloosterman sums assume modulo 18 and 54. The proofs use Stickelberger's theorem, the Gross-Koblitz formula and Fourier analysis.

Keywords: Kloosterman sums, Stickelberger's theorem, Gross-Koblitz formula

1 Introduction

Let $\mathcal{K}_{p^n}(a)$ denote the p -ary Kloosterman sum defined by

$$\mathcal{K}_{p^n}(a) := \sum_{x \in \mathbb{F}_{p^n}} \zeta^{\text{Tr}(x^{p^n-2} + ax)},$$

for any $a \in \mathbb{F}_{p^n}$, where ζ is a primitive p -th root of unity and Tr denotes the absolute trace map $\text{Tr} : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$ defined as usual as

$$\text{Tr}(c) := c + c^p + c^{p^2} + \cdots + c^{p^{n-1}}.$$

Kloosterman sums have attracted attention thanks to their various links to other related fields. For instance, a zero of a binary Kloosterman sum on \mathbb{F}_{2^n} leads to a bent function from

*Research supported by Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006

†Research supported by Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006, and the Irish Research Council for Science, Engineering and Technology

$\mathbb{F}_{2^{2n}} \rightarrow \mathbb{F}_2$ as proven by Dillon in [2]. Similarly, zeros of ternary Kloosterman sums give rise to ternary bent functions [6]. However determining a zero of a Kloosterman sum is not easy. A recent result in this direction is the following: a binary or ternary Kloosterman sum $\mathcal{K}_{p^n}(a)$ is not zero if a is in a proper subfield of \mathbb{F}_{p^n} except when $p = 2, n = 4, a = 1$, see [14]. Given the difficulty of the problem of finding zeros (or explicit values) of Kloosterman sums, and that they sometimes do not exist, one is generally satisfied with divisibility results and characterisation of Kloosterman sums modulo some integer (see [15, 13, 3, 1, 14]).

It is easy to see that binary Kloosterman sums are divisible by $4 = 2^2$, i.e., for all $a \in \mathbb{F}_{2^n}$,

$$\mathcal{K}_{2^n}(a) \equiv 0 \pmod{4}. \quad (1)$$

They also satisfy (see [10])

$$-2^{n/2+1} \leq \mathcal{K}_{2^n}(a) \leq 2^{n/2+1},$$

and take every value which is congruent to 0 modulo 4 in that range.

Helleseth and Zinoviev proved the following result which improved (1) one level higher, i.e., modulo 2^3 , in the sense of describing the a for which $\mathcal{K}_{2^n}(a)$ is 0 or 4 modulo 8.

Theorem 1. [7] For $a \in \mathbb{F}_{2^n}$,

$$\mathcal{K}_{2^n}(a) \equiv \begin{cases} 0 \pmod{8} & \text{if } \text{Tr}(a) = 0, \\ 4 \pmod{8} & \text{if } \text{Tr}(a) = 1. \end{cases}$$

Similar to the binary case, it is easy to see that ternary Kloosterman sums are divisible by 3, i.e., for all $a \in \mathbb{F}_{3^n}$,

$$\mathcal{K}_{3^n}(a) \equiv 0 \pmod{3}. \quad (2)$$

Ternary Kloosterman sums satisfy (see Katz and Livné [8])

$$-2\sqrt{3^n} < \mathcal{K}_{3^n}(a) < 2\sqrt{3^n}$$

and take every value which is congruent to 0 modulo 3 in that range.

We will prove the following theorem, a simple characterisation of ternary Kloosterman sums modulo 3^2 using the trace map (similar to Helleseth-Zinoviev result for binary case), by using Stickelberger's theorem.

Theorem 2. For $a \in \mathbb{F}_{3^n}$,

$$\mathcal{K}_{3^n}(a) \equiv \begin{cases} 0 \pmod{9} & \text{if } \text{Tr}(a) = 0, \\ 3 \pmod{9} & \text{if } \text{Tr}(a) = 1, \\ 6 \pmod{9} & \text{if } \text{Tr}(a) = 2. \end{cases}$$

This result is implied by a result of van der Geer and van der Vlugt [18].

We will also give a characterisation modulo 3^3 of Kloosterman sums, using the Gross-Koblitz formula. The characterisation will depend on a generalisation of the trace function. Note that the trace of an element $a \in \mathbb{F}_q$ can be written as

$$\text{Tr}(a) := \sum_{i \in W_1} a^i,$$

where $W_1 := \{p^i \mid i \in \{0, \dots, n-1\}\}$. We will use a generalised trace $\tau_S : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$,

$$\tau_S(a) := \sum_{i \in S} a^i,$$

where S can be assigned to any subset of $\{0, \dots, p^n - 2\}$ satisfying

$$S^p := \{s^p \pmod{p^n - 1} \mid s \in S\} = S,$$

particularly quadratic and cubic powers of p , in contrast to the set of linear powers W_1 .

We will define the sets

$$\begin{aligned} X &:= \{r \in \{0, \dots, q-2\} \mid r = 3^i + 3^j\}, \text{ } (i, j \text{ not necessarily distinct}) \\ Y &:= \{r \in \{0, \dots, q-2\} \mid r = 3^i + 3^j + 3^k, i, j, k \text{ distinct}\}, \\ Z &:= \{r \in \{0, \dots, q-2\} \mid r = 2 \cdot 3^i + 3^j, i \neq j\}. \end{aligned}$$

Our main result is

Theorem 3. *Let $n \geq 3$, and let $q = 3^n$. Then*

$$\mathcal{K}_q(a) \equiv \begin{cases} 0 & \pmod{27} \text{ if } \text{Tr}(a) = 0 \text{ and } \tau_Y(a) + 2\tau_X(a) = 0 \\ 3 & \pmod{27} \text{ if } \text{Tr}(a) = 1 \text{ and } \tau_Y(a) = 2 \\ 6 & \pmod{27} \text{ if } \text{Tr}(a) = 2 \text{ and } \tau_Y(a) + \tau_X(a) = 2 \\ 9 & \pmod{27} \text{ if } \text{Tr}(a) = 0 \text{ and } \tau_Y(a) + 2\tau_X(a) = 1 \\ 12 & \pmod{27} \text{ if } \text{Tr}(a) = 1 \text{ and } \tau_Y(a) = 0 \\ 15 & \pmod{27} \text{ if } \text{Tr}(a) = 2 \text{ and } \tau_Y(a) + \tau_X(a) = 0 \\ 18 & \pmod{27} \text{ if } \text{Tr}(a) = 0 \text{ and } \tau_Y(a) + 2\tau_X(a) = 2 \\ 21 & \pmod{27} \text{ if } \text{Tr}(a) = 1 \text{ and } \tau_Y(a) = 1 \\ 24 & \pmod{27} \text{ if } \text{Tr}(a) = 2 \text{ and } \tau_Y(a) + \tau_X(a) = 1. \end{cases}$$

Recently, we have proved a similar result for the binary case, using τ_Q , where $Q := \{2^i + 2^j \mid i, j \in \{0, \dots, n-1\}, i \neq j\}$.

Theorem 4. [4] For $a \in \mathbb{F}_{2^n}$,

$$\mathcal{K}_{2^n}(a) \equiv \begin{cases} 0 \pmod{16} & \text{if } \text{Tr}(a) = 0 \text{ and } \tau_Q(a) = 0, \\ 4 \pmod{16} & \text{if } \text{Tr}(a) = 1 \text{ and } \tau_Q(a) = 1, \\ 8 \pmod{16} & \text{if } \text{Tr}(a) = 0 \text{ and } \tau_Q(a) = 1, \\ 12 \pmod{16} & \text{if } \text{Tr}(a) = 1 \text{ and } \tau_Q(a) = 0. \end{cases}$$

For the ternary case we mention a recent result due to Lisonek [13] that gives a description of the elements $a \in \mathbb{F}_{3^n}$ for which $\mathcal{K}(a) \equiv 0 \pmod{9}$, which is also implied by the van der Geer-van der Vlugt result.

Theorem 5. [13] Let $n \geq 2$. For any $a \in \mathbb{F}_{3^n}$, $\mathcal{K}_{3^n}(a)$ is divisible by 9 if and only if $\text{Tr}(a) = 0$.

In Sections 2 and 3, we will introduce the techniques we use. In Section 4 we will give the results modulo 9. In Section 5 we will give the modulo 27 result.

2 Stickelberger's theorem

Let p be a prime (in Section 4 we set $p = 3$). Consider multiplicative characters taking their values in an algebraic extension of \mathbb{Q}_p . Let ξ be a primitive $(q-1)^{\text{th}}$ root of unity in a fixed algebraic closure of \mathbb{Q}_p . The group of multiplicative characters of \mathbb{F}_q (denoted $\widehat{\mathbb{F}_q^\times}$) is cyclic of order $q-1$. The group $\widehat{\mathbb{F}_q^\times}$ is generated by the Teichmüller character $\omega : \mathbb{F}_q \rightarrow \mathbb{Q}_p(\xi)$, which, for a fixed generator t of \mathbb{F}_q^\times , is defined by $\omega(t^j) = \xi^j$. We set $\omega(0)$ to be 0. An equivalent definition is that ω satisfies

$$\omega(a) \equiv a \pmod{p}$$

for all $a \in \mathbb{F}_q$.

Let ζ be a fixed primitive p -th root of unity in the fixed algebraic closure of \mathbb{Q}_p . Let μ be the canonical additive character of \mathbb{F}_q ,

$$\mu(x) = \zeta^{\text{Tr}(x)}$$

where Tr denotes the absolute trace map from \mathbb{F}_q to \mathbb{F}_p .

The Gauss sum (see [12, 20]) of a character $\chi \in \widehat{\mathbb{F}_q^\times}$ is defined as

$$\tau(\chi) = - \sum_{x \in \mathbb{F}_q} \chi(x) \mu(x).$$

We define

$$g(j) := \tau(\omega^{-j}).$$

For any positive integer j , let $\text{wt}_p(j)$ denote the p -weight of j , i.e.,

$$\text{wt}_p(j) = \sum_i j_i$$

where $\sum_i j_i p^i$ is the p -ary expansion of j .

Let π be the unique $(p-1)$ th root of $-p$ in $\mathbb{Q}_p(\xi, \zeta)$ satisfying

$$\pi \equiv \zeta - 1 \pmod{\pi^2}.$$

Wan [19] noted that the following improved version of Stickelberger's theorem is a direct consequence of the Gross-Koblitz formula (see Section 5).

Theorem 6. [19] *Let $1 \leq j < q-1$ and let $j = j_0 + j_1 p + \cdots + j_{n-1} p^{n-1}$. Then*

$$g(j) \equiv \frac{\pi^{\text{wt}_p(j)}}{j_0! \cdots j_{n-1}!} \pmod{\pi^{\text{wt}_p(j)+p-1}}.$$

Stickelberger's theorem, as usually stated, is the same congruence modulo $\pi^{\text{wt}_p(j)+1}$.

We have (see [5]) that (π) is the unique prime ideal of $\mathbb{Q}_p(\zeta, \xi)$ lying above p . Since $\mathbb{Q}_p(\zeta, \xi)$ is an unramified extension of $\mathbb{Q}_p(\zeta)$, a totally ramified (degree $p-1$) extension of \mathbb{Q}_p , it follows that $(\pi)^{p-1} = (p)$ and $\nu_p(\pi) = \frac{1}{p-1}$. Here ν_p denotes the p -adic valuation.

Therefore Theorem 6 implies that $\nu_\pi(g(j)) = \text{wt}_p(j)$, and because $\nu_p(g(j)) = \nu_\pi(g(j)) \cdot \nu_p(\pi)$ we get

$$\nu_p(g(j)) = \frac{\text{wt}_p(j)}{p-1}. \quad (3)$$

In this paper we have $p = 3$. In that case, $\pi = -2\zeta - 1$ and $\pi^2 = -3$. Hence (3) becomes

$$\nu_3(g(j)) = \frac{\text{wt}_3(j)}{2}. \quad (4)$$

3 Fourier coefficients

The Fourier transform of a function $f : \mathbb{F}_q \rightarrow \mathbb{C}$ at $a \in \mathbb{F}_q$ is defined to be

$$\widehat{f}(a) = \sum_{x \in \mathbb{F}_q} f(x) \mu(ax).$$

The complex number $\widehat{f}(a)$ is called the Fourier coefficient of f at a .

Consider monomial functions defined by $f(x) = \mu(x^d)$. When $d = -1$ we have $\widehat{f}(a) = \mathcal{K}_{p^n}(a)$. By a similar Fourier analysis argument to that in Katz [9] or Langevin-Leander [11], for any d we have

$$\widehat{f}(a) = \frac{q}{q-1} + \frac{1}{q-1} \sum_{j=1}^{q-2} \tau(\bar{\omega}^j) \tau(\omega^{jd}) \bar{\omega}^{jd}(a)$$

and hence

$$\widehat{f}(a) \equiv - \sum_{j=1}^{q-2} \tau(\bar{\omega}^j) \tau(\omega^{jd}) \bar{\omega}^{jd}(a) \pmod{q}.$$

We will use this to obtain congruence information about Kloosterman sums. Putting $d = -1 = p^n - 2$, the previous congruence becomes

$$\mathcal{K}(a) \equiv - \sum_{j=1}^{q-2} (g(j))^2 \omega^j(a) \pmod{q}. \quad (5)$$

In this paper, $p = 3$. Equation (4) gives the 3-adic valuation of the Gauss sums $g(j)$, and the 3-adic valuation of each term in equation (5) follows. Our proofs will consider (5) at various levels, i.e., modulo 3^2 and 3^3 .

4 Ternary Kloosterman sums modulo 9

In this section we will prove our result using Stickelberger's theorem. First we need a lemma which helps us in our proof.

Lemma 7. *Let p be a prime, $q = p^n$ and $r \in \mathbb{F}_p^\times$. If T_r denotes the set $\{a \in \mathbb{F}_q \mid \text{Tr}(a) = r\}$, then*

$$\sum_{t \in T_r} t^{-1} = r^{-1}.$$

Proof. Consider the polynomials

$$g(x) = \prod_{t \in T_r} (x - t),$$

$$h(x) = \prod_{t \in T_r} (x - t^{-1}).$$

Note that $g(x)$ vanishes on the p^{n-1} elements of T_r . Thus

$$g(x) = x^{p^{n-1}} + x^{p^{n-2}} + \cdots + x - r.$$

In particular,

$$\prod_{t \in T_r} (-t) = -r,$$

so

$$\prod_{t \in T_r} (-t^{-1}) = -r^{-1}.$$

The reciprocal polynomial of g is $g^*(x) = x^{p^{n-1}}g(1/x)$.

We therefore get

$$\begin{aligned} h(x) &= -r^{-1}g^*(x) \\ &= -r^{-1}x^{p^{n-1}}g(1/x) \\ &= x^{p^{n-1}} - r^{-1}x^{p^{n-1}-1} - \cdots - r^{-1}x^{p^{n-1}-p^{n-2}} - r^{-1}. \end{aligned}$$

Thus

$$\sum_{t \in T_r} (-t^{-1}) = -r^{-1}.$$

□

From now on, we set $p = 3$, so that $\mathcal{K}_q(a)$ is an integer for $a \in \mathbb{F}_q$. Since there will not be any confusion with binary Kloosterman sums we will write $\mathcal{K}(a)$ for $\mathcal{K}_q(a)$. We consider the function $f(x) = \mu(x^{-1}) = \mu(x^{q-2})$. Then $\widehat{f}(a)$ is the Kloosterman sum $\mathcal{K}(a)$. The following lemma will be needed.

Lemma 8. *Let $q = 3^n$, and T_1 be as defined above. Then*

$$\sum_{z \in T_1} \bar{\omega}(z) \equiv 1 \pmod{3}.$$

Proof. Follows directly from Lemma 7 and the definition of the Teichmüller character. □

We can now state our main result of this section.

Theorem 9. *Let $q = 3^n$ for some integer $n > 1$. For $a \in \mathbb{F}_q$,*

$$\mathcal{K}_q(a) \equiv \begin{cases} 0 & \pmod{9} & \text{if } \text{Tr}(a) = 0, \\ 3 & \pmod{9} & \text{if } \text{Tr}(a) = 1, \\ 6 & \pmod{9} & \text{if } \text{Tr}(a) = 2. \end{cases}$$

Proof. By (5)

$$\mathcal{K}(a) \equiv - \sum_{j=1}^{q-2} g(j)^2 \omega^j(a) \pmod{q}. \quad (6)$$

Let, for any $0 < t < q - 1$, the 3-adic expansion of t be $t = t_0 + 3t_1 + \cdots + 3^{n-1}t_{n-1}$ and let \mathcal{P} be the prime of $\mathbb{Q}_3(\xi, \zeta)$ lying above 3. As we mentioned in Section 2, Stickelberger's theorem implies that

$$\begin{aligned} \nu_{\mathcal{P}}(g(t)) &= \text{wt}_3(t) = t_0 + t_1 + \cdots + t_{n-1} \\ \nu_3(g(t)) &= \frac{\text{wt}_3(t)}{2}, \\ \text{and so } \nu_3((g(t))^2) &= \text{wt}_3(t). \end{aligned} \quad (7)$$

Now (7) implies that any term in the sum in (6) with $\text{wt}_3(j) > 1$ will be 0 modulo 9, so (6) modulo 9 becomes a sum over terms of weight 1 only:

$$\mathcal{K}(a) \equiv - \sum_{0 \leq i < n} g(3^i)^2 \omega^{3^i}(a) \pmod{9}.$$

By Lemma 6.5 of [20], $g(3^i) = g(1)$, so we obtain

$$\mathcal{K}(a) \equiv -g(1)^2 \sum_{0 \leq i < n} \omega^{3^i}(a) \pmod{9}. \quad (8)$$

By definition of ω , we have

$$\sum_{0 \leq i < n} \omega^{3^i}(a) \equiv \text{Tr}(a) \pmod{3}. \quad (9)$$

Since $\nu_3(g(1)^2) = \text{wt}_3(1) = 1$, the proof of the theorem reduces to determining $g(1)^2 \pmod{9}$. We calculate, using the notation of Lemma 7,

$$\begin{aligned} g(1) &= - \sum_{x \in \mathbb{F}_q^\times} \bar{\omega}(x) \zeta^{\text{Tr}(x)} \\ &= - \sum_{x \in T_0} \bar{\omega}(x) - \sum_{x \in T_1} \bar{\omega}(x) \zeta - \sum_{x \in T_1} \bar{\omega}(-x) \zeta^2 \\ &= (\zeta^2 - \zeta) \sum_{x \in T_1} \bar{\omega}(x) \end{aligned}$$

because $\bar{\omega}(-x) = -\bar{\omega}(x)$, $T_2 = -T_1$, and the sum over T_0 is 0. This implies

$$g(1)^2 = (\zeta^2 - \zeta)^2 \left(\sum_{x \in T_1} \bar{\omega}(x) \right)^2.$$

But we have $(\zeta^2 - \zeta)^2 = -3$. This, together with Lemma 8, implies

$$g(1)^2 \equiv 6 \pmod{9}. \quad (10)$$

Combining this with (9), the congruence (8) becomes

$$\mathcal{K}(a) \equiv 3 \operatorname{Tr}(a) \pmod{9}$$

as required. \square

Garaschuk and Lisonek proves the following theorem which characterises ternary Kloosterman sums modulo 2.

Theorem 10. [14] *Let \sqrt{a} denote any $b \in \mathbb{F}_{3^n}$ such that $b^2 = a$.*

$$\mathcal{K}_{3^n}(a) \equiv \begin{cases} 0 \pmod{2} & \text{if } a = 0 \text{ or } a \text{ is a square and } \operatorname{Tr}(\sqrt{a}) \neq 0, \\ 1 \pmod{2} & \text{otherwise.} \end{cases}$$

Theorem 9 and Theorem 10 together give a full characterisation of ternary Kloosterman sums modulo 18, which we summarise in the following corollary.

Corollary 11. *Let $q = 3^n$. For $a \in \mathbb{F}_q^\times$,*

$$\mathcal{K}_q(a) \equiv \begin{cases} 0 \pmod{18} & \text{if } \operatorname{Tr}(a) = 0 \text{ and } a \text{ square with } \operatorname{Tr}(\sqrt{a}) \neq 0, \\ 3 \pmod{18} & \text{if } \operatorname{Tr}(a) = 1 \text{ and } a \text{ non-square or } \operatorname{Tr}(\sqrt{a}) = 0, \\ 6 \pmod{18} & \text{if } \operatorname{Tr}(a) = 2 \text{ and } a \text{ square with } \operatorname{Tr}(\sqrt{a}) \neq 0, \\ 9 \pmod{18} & \text{if } \operatorname{Tr}(a) = 0 \text{ and } a \text{ non-square or } \operatorname{Tr}(\sqrt{a}) = 0, \\ 12 \pmod{18} & \text{if } \operatorname{Tr}(a) = 1 \text{ and } a \text{ square with } \operatorname{Tr}(\sqrt{a}) \neq 0, \\ 15 \pmod{18} & \text{if } \operatorname{Tr}(a) = 2 \text{ and } a \text{ non-square or } \operatorname{Tr}(\sqrt{a}) = 0. \end{cases}$$

5 Ternary Kloosterman sums modulo 27

To be able to give higher level congruences we will need a result stronger than Stickelberger's theorem. Recall that Gauss sums lie in $\mathbb{Z}_p[\zeta, \xi]$, and that (π) is the unique prime ideal of $\mathbb{Z}_p[\zeta, \xi]$ lying above p . All congruences involving Gauss sums take place in this ring, so when we write $g(j)^2 \equiv 6 \pmod{27}$ we mean that $g(j)^2 - 6$ is in the ideal (27). The

Gross-Koblitz formula [5, 17] states that

$$g(j) = \pi^{\operatorname{wt}_p(j)} \prod_{i=0}^{n-1} \Gamma_p \left(\left\langle \frac{p^i j}{q-1} \right\rangle \right) \quad (11)$$

where $\langle x \rangle$ is the fractional part of a rational number x , and Γ_p is the p -adic Gamma function $\Gamma_p : \mathbb{N} \rightarrow \mathbb{N}$ defined by (cf. [16])

$$\Gamma_p(k) = (-1)^k \prod_{\substack{t < k \\ (t,p)=1}} t.$$

The following result helps one computing the p -adic Gamma function modulo p^k .

Theorem 12 (Generalised Wilson's theorem). [16]

Suppose $x \equiv y \pmod{p^k}$. If $p^k \neq 4$, then

$$\Gamma_p(x) \equiv \Gamma_p(y) \pmod{p^k}.$$

This theorem is actually a consequence of Gauss' generalisation of Wilson's theorem. Now let us prove a lemma on evaluations of the p -adic Gamma function. This lemma will allow us to evaluate Gauss sums for higher moduli and find Kloosterman congruences modulo 27.

Lemma 13. Let $q = 3^n$ and let i be an integer in the range $[0, n-1]$. Then

$$\Gamma_3 \left(\left\langle \frac{3^i}{q-1} \right\rangle \right) \equiv \begin{cases} 13 \pmod{27} & \text{if } i = 1, \\ 1 \pmod{27} & \text{if } i > 1. \end{cases}$$

Proof. For any j , we have $3^j \leq q$, and

$$\left\langle \frac{3^i}{q-1} \right\rangle = \frac{3^i}{q-1} \equiv 3^i(3^j - 1) \pmod{3^j},$$

so

$$\Gamma_3 \left(\left\langle \frac{3^i}{q-1} \right\rangle \right) \equiv \Gamma_3(26 \cdot 3^i) \pmod{27}.$$

If $i \geq 3$, then $26 \cdot 3^i \equiv 0 \pmod{27}$, and

$$\Gamma_3 \left(\left\langle \frac{3^i}{q-1} \right\rangle \right) \equiv 1 \pmod{27},$$

Now $\Gamma_3(26 \cdot 3) \equiv \Gamma_3(24) \pmod{27}$ using Generalised Wilson's theorem. And $\Gamma_3(24) \equiv 13 \pmod{9}$. Similarly:

$$\Gamma_3(26 \cdot 9) \equiv 1 \pmod{27}.$$

□

Lemma 13 allows us to compute Gauss sums modulo 27:

Lemma 14. *Let $q = 3^n$. Then*

$$g(j)^2 \equiv \begin{cases} 6 \pmod{27} & \text{if } \text{wt}_p(j) = 1, \\ 9 \pmod{27} & \text{if } \text{wt}_p(j) = 2, \\ 0 \pmod{27} & \text{if } \text{wt}_p(j) \geq 3. \end{cases}$$

Proof. Suppose $\text{wt}_p(j) = 1$. By the Gross-Koblitz formula and Lemma 13,

$$g(j) \equiv 13\pi \pmod{27}.$$

Let

$$g(j) = 27A + 13\pi$$

for some $A \in \mathbb{Z}_p[\zeta, \xi]$. Then

$$\begin{aligned} g(j)^2 &= 27^2 A^2 + 2 \cdot 27 \cdot 13A + 169\pi^2 \\ &\equiv 169\pi^2 \pmod{27} \\ &\equiv 6 \pmod{27} \end{aligned}$$

since $\pi^2 = -3$. Now suppose $\text{wt}_p(j) = 2$. By the Gross-Koblitz formula,

$$g(j) \equiv -3 \pmod{9}.$$

Thus $g(j) = 9X - 3$ for some $X \in \mathbb{Z}_p[\zeta, \xi]$, so

$$g(j)^2 = 81X^2 - 54X + 9 \equiv 9 \pmod{27}.$$

It is clear from the Gross-Koblitz formula that if $\text{wt}_p(j) > 2$, then

$$27|\pi^{2\text{wt}_p(j)}|g(j)^2.$$

□

Consider again the trace function $\text{Tr} : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$,

$$\text{Tr}(c) = c + c^p + c^{p^2} + \cdots + c^{p^{n-1}}.$$

We wish to generalise this definition to a larger class of finite field sums, which includes the usual trace function as a special case.

Definition 1. Let p be a prime, let $n \geq 1$ be an integer and let $q = p^n$. For any $S \subseteq \mathbb{Z}/(q-1)\mathbb{Z}$ satisfying $S^p = S$ where $S^p := \{s^p \mid s \in S\}$, define the S -trace to be the function $\tau_S : \mathbb{F}_q \rightarrow \mathbb{F}_p$,

$$\tau_S(c) := \sum_{s \in S} c^s.$$

Let

$$\begin{aligned} X &:= \{r \in \{0, \dots, q-2\} | r = 3^i + 3^j\}, \text{ } (i, j \text{ not necessarily distinct}) \\ Y &:= \{r \in \{0, \dots, q-2\} | r = 3^i + 3^j + 3^k, i, j, k \text{ distinct}\}, \\ Z &:= \{r \in \{0, \dots, q-2\} | r = 2 \cdot 3^i + 3^j, i \neq j\}. \end{aligned}$$

Now we are ready to prove our result on Kloosterman sums modulo 27.

Theorem 15. *Let \mathcal{K}_q be the usual q -ary Kloosterman sum, let*

$$\widehat{\text{Tr}}(a) = \sum_{\text{wt}_3(i)=1} \omega^i(a), \text{ and let } \widehat{\tau}_X(a) = \sum_{\text{wt}_3(j)=2} \omega^j(a).$$

Then

$$\mathcal{K}_{3^n}(a) \equiv 21\widehat{\text{Tr}}(a) + 18\widehat{\tau}_X(a) \pmod{27}. \quad (12)$$

Proof. Using (5) and Lemma 14, we get

$$\begin{aligned} \mathcal{K}(a) &\equiv - \sum_{j=1}^{q-2} g(j)^2 \omega^j(a) \pmod{q} \\ &\equiv - \sum_{\text{wt}_3(j)=1} g(j)^2 \omega^j(a) - \sum_{\text{wt}_3(j)=2} g(j)^2 \omega^j(a) \pmod{27} \\ &\equiv -6 \sum_{\text{wt}_3(j)=1} \omega^j(a) - 9 \sum_{\text{wt}_3(j)=2} \omega^j(a) \pmod{27} \\ &\equiv 21\widehat{\text{Tr}}(a) + 18\widehat{\tau}_X(a) \pmod{27}. \quad \square \end{aligned}$$

It would be preferable to express the above result in terms of operations within \mathbb{F}_q itself. Note that in (12) we only need $\widehat{\text{Tr}}(a)$ modulo 9 and $\widehat{\tau}_X(a)$ modulo 3. We have

$$\tau_X(a) \equiv \widehat{\tau}_X(a) \pmod{3}.$$

We need to find some condition for $\widehat{\text{Tr}}(a)$ modulo 9 using functions from \mathbb{F}_q to \mathbb{F}_p . We will do that in the proof of the following corollary.

Corollary 16. *Let $n \geq 3$, and let $q = 3^n$. Then*

$$\mathcal{K}_q(a) \equiv 21 \text{Tr}(a)^3 + 18\tau_Z(a) + 9\tau_Y(a) + 18\tau_X(a) \pmod{27}.$$

Proof. First note that $\widehat{Q}(a) \equiv \tau_X(a) \pmod{3}$, by the basic property of the Teichmüller character.

To determine $\widehat{\text{Tr}}(a) \pmod{9}$, we compute

$$\begin{aligned}\widehat{\text{Tr}}(a)^3 &= \sum_{i,j,k \in \{0, \dots, n-1\}} \omega(a^{3^i+3^j+3^k}) \\ &= \widehat{\text{Tr}}(a) + 3 \sum_{r \in Z} \omega(a^r) + 6 \sum_{r \in Y} \omega(a^r),\end{aligned}$$

and note the elementary fact that if $x \equiv y \pmod{m}$, then $x^m \equiv y^m \pmod{m^2}$. This means that $\widehat{\text{Tr}}(a)^3 \pmod{9}$ is given by $\widehat{\text{Tr}}(a) \pmod{3} = \text{Tr}(a)$, i.e. $\widehat{\text{Tr}}(a)^3 \pmod{9} = \text{Tr}(a)^3$.

Since

$$\sum_{r \in Z} \omega(a^r) \equiv \tau_Z(a) \pmod{3}$$

and

$$\sum_{r \in Y} \omega(a^r) \equiv \tau_Y(a) \pmod{3},$$

we have that

$$\widehat{\text{Tr}}(a) \equiv \text{Tr}(a)^3 - 3\tau_Z(a) - 6\tau_Y(a) \pmod{9},$$

proving the result. □

Note that

$$\text{Tr}(a)\tau_X(a) = \text{Tr}(a) + 2\tau_Z(a).$$

Thus Corollary 16 can be rewritten as

$$\mathcal{K}_q(a) \equiv 21 \text{Tr}(a)^3 + 18 \text{Tr}(a) + 18\tau_X(a) + 9 \text{Tr}(a)\tau_X(a) + 9\tau_Y(a) \pmod{27}. \quad (13)$$

The smallest field for which each of the 27 possible values of $(\text{Tr}(a), \tau_X(a), \tau_Y(a))$ occurs is \mathbb{F}_{3^6} .

Corollary 17. *Let $n \geq 3$, and let $q = 3^n$. Then*

$$\mathcal{K}_q(a) \equiv \begin{cases} 0 & \pmod{27} \text{ if } \text{Tr}(a) = 0 \text{ and } \tau_Y(a) + 2\tau_X(a) = 0 \\ 3 & \pmod{27} \text{ if } \text{Tr}(a) = 1 \text{ and } \tau_Y(a) = 2 \\ 6 & \pmod{27} \text{ if } \text{Tr}(a) = 2 \text{ and } \tau_Y(a) + \tau_X(a) = 2 \\ 9 & \pmod{27} \text{ if } \text{Tr}(a) = 0 \text{ and } \tau_Y(a) + 2\tau_X(a) = 1 \\ 12 & \pmod{27} \text{ if } \text{Tr}(a) = 1 \text{ and } \tau_Y(a) = 0 \\ 15 & \pmod{27} \text{ if } \text{Tr}(a) = 2 \text{ and } \tau_Y(a) + \tau_X(a) = 0 \\ 18 & \pmod{27} \text{ if } \text{Tr}(a) = 0 \text{ and } \tau_Y(a) + 2\tau_X(a) = 2 \\ 21 & \pmod{27} \text{ if } \text{Tr}(a) = 1 \text{ and } \tau_Y(a) = 1 \\ 24 & \pmod{27} \text{ if } \text{Tr}(a) = 2 \text{ and } \tau_Y(a) + \tau_X(a) = 1. \end{cases}$$

Proof. Restatement of equation 13. □

The Kloosterman sums modulo 54 can be given by combining (16) and Theorem 10.

References

- [1] Pascale Charpin, Tor Helleseth, and Victor Zinoviev. The divisibility modulo 24 of Kloosterman sums on $GF(2^m)$, m odd. *Journal of Combinatorial Theory*, 114:332–338, 2007.
- [2] J. F. Dillon. *Elementary Hadamard Difference Sets*. PhD thesis, University of Maryland, 1974.
- [3] Kseniya Garaschuk and Petr Lisoněk. On binary Kloosterman sums divisible by 3. *Designs, Codes and Cryptography*, 49:347–357, 2008.
- [4] Faruk Göloğlu, Gary McGuire, and Richard Moloney. Binary Kloosterman sums using Stickelberger’s theorem and the Gross-Koblitz formula. Submitted, 2010.
- [5] Benedict H. Gross and Neal Koblitz. Gauss sums and the p -adic Γ -function. *Ann. of Math. (2)*, 109(3):569–581, 1979.
- [6] Tor Helleseth and Alexander Kholosha. Monomial and quadratic bent functions over the finite fields of odd characteristic. *IEEE Trans. Inform. Theory*, 52(5):2018–2032, 2006.
- [7] Tor Helleseth and Victor Zinoviev. On \mathbb{Z}_4 -linear Goethals codes and Kloosterman sums. *Designs, Codes and Cryptography*, 17:269–288, 1999.
- [8] Nicholas Katz and Ron Livné. Sommes de Kloosterman et courbes elliptiques universelles caractéristiques 2 et 3. *C. R. Acad. Sci. Paris Sér. I Math.*, 309(11):723–726, 1989.
- [9] Nicholas M. Katz. *Gauss sums, Kloosterman sums, and monodromy groups*, volume 116 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1988.
- [10] G. Lachaud and J. Wolfmann. The weights of the orthogonals of the extended quadratic binary Goppa codes. *IEEE Trans. Inform. Theory*, 36(3):686–692, 1990.
- [11] Philippe Langevin and Gregor Leander. Monomial bent functions and Stickelberger’s theorem. *Finite Fields and Their Applications*, 14:727–742, 2008.
- [12] Rudolf Lidl and Harald Niederreiter. *Introduction to Finite Fields and Their Applications*. Cambridge University Press, 1986.

- [13] Petr Lisoněk. On the connection between Kloosterman sums and elliptic curves. In Solomon W. Golomb, Matthew G. Parker, Alexander Pott, and Arne Winterhof, editors, *SETA*, volume 5203 of *Lecture Notes in Computer Science*, pages 182–187. Springer, 2008.
- [14] Petr Lisoněk and Marko Moisio. On zeros of Kloosterman sums. To appear, 2009.
- [15] Marko Moisio. The divisibility modulo 24 of Kloosterman sums on $GF(2^m)$, m even. *Finite Fields and Their Applications*, 15:174–184, 2009.
- [16] Yasuo Morita. A p -adic analogue of the Γ -function. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 22(2):255–266, 1975.
- [17] Alain Robert. The Gross-Koblitz formula revisited. *Rendiconti del Seminario Matematico della Università di Padova*, 105:157 – 170, 2001.
- [18] Gerard van der Geer and Marcel van der Vlugt. Kloosterman sums and the p -torsion of certain Jacobians. *Math. Ann.*, 290(3):549–563, 1991.
- [19] Da Qing Wan. Minimal polynomials and distinctness of Kloosterman sums. *Finite Fields Appl.*, 1(2):189–203, 1995. Special issue dedicated to Leonard Carlitz.
- [20] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Springer, 1982.